兵庫県警察情報セキュリティ対策基準（例規甲）

〔平成23年２月23日
兵警情例規甲第１号〕

兵庫県警察情報セキュリティ対策基準を下記のように定め、平成23年３月１日から実施する。

記

第１　総則

１　趣旨

この対策基準は、兵庫県警察情報セキュリティに関する訓令（平成23年兵庫県警察本部訓令第１号。以下「訓令」という。）第５条第２項の規定に基づき、本県警察における警察情報システム等において取り扱う情報の分類及び情報セキュリティを維持するための対策の基準に関し必要な事項を定めるものとする。

２　定義規定等の適用

訓令に定めるところによる定義規定及び略称規定は、この対策基準において適用する。

３　定義

この対策基準において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　兵庫県警察情報セキュリティポリシー　訓令及び訓令に基づく規程に規定された情報セキュリティに関する事項をいう。

(2)　入出力資料　警察情報システム等に入力された又は警察情報システム等により出力された情報を記録した文書、図画及び電磁的記録（作成中のものを含む。）をいう。

(3)　ドキュメント　警察情報システムに関する文書、図画及び電磁的記録（作成中のものを含む。）で、システムドキュメント及び取扱説明書（システムを利用する者が業務を行う上で参照する機器の操作の方法を説明した記録をいう。）をいう。

(4)　システムドキュメント　ドキュメントのうち、次に掲げるものをいう。

ア　システム仕様書（情報の処理に必要な機能、項目等を定義した記録をいう。）

イ　システム設計書（情報の処理手順並びに機器及びプログラムの構成の概要の記録をいう。）

ウ　プログラム仕様書（情報の処理手順の概要の記録をいう。）

エ　プログラムリスト（情報の処理手順を電子計算機に指示した記録をいう。）

オ　操作指示書（システムの維持管理に伴う機器の設定方法等を説明した記録をいう。）

(5)　外部記録媒体　フロッピーディスク、フラッシュメモリ、光ディスク等警察情報システム等に接続し情報を入出力する電磁的記録媒体をいう。
(6)　情報　入出力資料、ドキュメント又は外部記録媒体若しくは警察情報システム等の内部に記録された情報をいう。
(7)　アクセス　警察情報システムにデータを入力し、又は警察情報システムからデータを出力することをいう。
(8)　アクセス権者　アクセスを行う権限を与えられた者をいう。
(9)　アクセス範囲　アクセス権者ごとにその者が行うことができるアクセスの範囲をいう。
(10)　ユーザＩＤ　アクセス権者を識別するためにアクセス権者ごとに付与された文字列をいう。
(11)　パスワード　警察情報システムを利用しようとする者がアクセス権者本人であるかどうかを検証するために用いられる文字列をいう。
(12)　認証　ユーザＩＤ、パスワード等を警察情報システムに入力することなどにより、警察情報システムを利用しようとする者がアクセス権者であるか否かを検証することをいう。
(13)　データベース装置　警察情報システムを構成するメインフレーム、サーバ等の電子計算機及びこれらに附置されるシステム管理を行う電子計算機をいう。
(14)　ネットワーク機器　警察情報システムを構成するルータ、レイヤ３スイッチ、スイッチングハブ等の機器若しくは伝送通信装置又はこれらから出力されるデータを利用することによりネットワークを管理する機能を有する機器をいう。
(15)　持ち出し用パソコン　警察情報システム等のうち、一の警察の庁舎内から移動して運用するものとして整備されたものをいう。
(16)　外部回線　警察機関の管理が及ばない電子計算機が論理的に接続され、当該電子計算機の通信に利用されるインターネットその他の電気通信回線をいう。

第２　管理体制

１　情報セキュリティ管理者

情報セキュリティ管理者は、警察情報システム等に係る情報セキュリティに関する事務を統括する。

２　情報セキュリティ副管理者

(1)　本部に、情報セキュリティ副管理者を置く。
(2)　情報セキュリティ副管理者は、総務部情報管理課長をもって充てる。
(3)　情報セキュリティ副管理者は、情報セキュリティ管理者を補佐する。

３　システムセキュリティ責任者

(1)　警察情報システム等の整備を担当する所属に、システムセキュリティ責任者を置く。
(2)　システムセキュリティ責任者は、当該所属の長をもって充てる。
(3)　システムセキュリティ責任者は、整備する警察情報システム等に関して、システムセキュリティ維持管理者及び運用管理責任者がそれぞれの事務を処理す

るに当たって必要な情報セキュリティ要件を当該警察情報システムが備えるための事務を処理するとともに、整備した警察情報システム等におけるシステムセキュリティ維持管理者が行う事務を統括する。

4　システムセキュリティ維持管理者

(1)　警察情報システムを構成する電子計算機及びネットワーク機器の管理者権限を保有する所属に、システムセキュリティ維持管理者を置く。

(2)　システムセキュリティ維持管理者は、当該所属の長をもって充てる。

(3)　システムセキュリティ維持管理者は、管理者権限を保有する電子計算機及びネットワーク機器に係る警察情報システムの維持管理をする際における情報セキュリティに係る事務を処理する。

5　システム管理担当者

(1)　システムセキュリティ維持管理者は、その管理する電子計算機ごとにシステム管理担当者を指定し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。

(2)　システム管理担当者は、担当する電子計算機その他の警察情報システムの情報セキュリティに係るシステム管理に関する事務を行う。

(3)　システム管理担当者は、同一の者が複数の電子計算機に関して重複して選任されることを妨げない。

6　ネットワーク管理担当者

(1)　システムセキュリティ維持管理者は、その管理するネットワーク機器ごとにネットワーク管理担当者を指定し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。ただし、ネットワーク機器の維持管理に係る事務が軽微であると認められるときは、当該事務をシステム管理担当者に行わせることができる。

(2)　ネットワーク管理担当者は、担当するネットワーク機器その他の警察情報システムに係るデータ伝送に関する監視及び制御その他の情報セキュリティに係るネットワーク管理に関する事務を行う。

(3)　ネットワーク管理担当者は、同一の者が複数のネットワーク機器に関して重複して選任されることを妨げない。

7　運用管理責任者

(1)　所属に、運用管理責任者を置く。

(2)　運用管理責任者は、所属長をもって充てる。

(3)　運用管理責任者は、所属における警察情報システム等の運用に関し、情報セキュリティの維持その他の警察情報システム等による処理に係る情報の適正な取扱いを確保するために必要な事務を処理する。

8　運用管理副責任者

(1)　所属に、運用管理副責任者を置く。

(2)　運用管理副責任者は、警察本部の所属（警察学校を含む。以下同じ。）にあっては次席、次長、副隊長又は副校長を、警察署にあっては副署長をもって充てる。

(3)　運用管理副責任者は、運用管理責任者を補佐するとともに、取扱責任者を指揮監督する。

9　取扱責任者

(1)　所属に、取扱責任者を置く。

(2)　取扱責任者は、警察本部の所属にあっては所属長補佐等（兵庫県警察における文書の管理に関する訓令（平成13年兵庫県警察本部訓令第14号）第２条第２号の所属長補佐等をいう。以下同じ。）を、警察署にあっては課長の職にある者をもって充てる。ただし、所属長は、必要があると認めるときは、所属長補佐等以外の者又は課長以外の者を取扱責任者に指定することができる。

(3)　所属長は、前記(2)の規定により、所属長補佐等以外の者又は課長以外の者を取扱責任者に指定したときは、事務担当者任免簿（兵庫県警察処務規程（昭和39年兵庫県警察本部訓令第６号）様式第10号）により、その状況を明らかにしておかなければならない。

(4)　取扱責任者は、運用管理責任者の指揮を受け、警察情報システム等の適正な運用を行う。

10　ＩＴ指導員

(1)　所属にＩＴ指導員を置く。

(2)　所属長は、次のいずれかの要件に該当する者のうちから優れた指導力を有する者をＩＴ指導員に指定するものとする。

ア　情報処理能力検定に関する訓令（平成５年警察庁訓令第１号）第３条に規定する中級又は上級の警察職員の情報処理能力についての検定に合格した者

イ　警察教養細則（平成13年警察庁訓令第４号）第５条第１項の規定に基づき行う情報管理専科の課程を修了した者

ウ　その他情報技術に係る優れた知識と能力を有する者

(3)　ＩＴ指導員の任務等については、総務部長が定める。

第３　情報の分類及び取扱い

１　情報の分類の基準

訓令第５条第１項の規定による情報の分類は、別表１のとおり行う。

２　分類が異なる情報の取扱い

機密性、完全性又は可用性のいずれかの情報の分類の区分が異なる情報を一の警察情報システム等において取り扱うことについては、次のいずれかに該当するときに限り認めるものとする。

(1)　当該警察情報システム等において取り扱う情報のうち、最も上位の分類の区分に応じた情報の管理が可能であるとき。

(2)　最高情報セキュリティ管理者（警察情報セキュリティに関する訓令（平成15年警察庁訓令第３号）第３条に規定する最高情報セキュリティ管理者をいう。以下同じ。）の承認を受けたとき。

３　情報の分類及び通知

(1)　情報セキュリティ管理者は、警察情報システム等において取り扱われる情報について、当該情報に係る業務を主管する所属の長及び当該情報を取り扱う警

察情報システムに係るシステムセキュリティ責任者と協議の上、分類するものとする。

(2)　情報セキュリティ管理者は、前記(1)の規定により分類した内容を関係所属の長に通知するものとする。

(3)　情報セキュリティ管理者は、情報の分類を変更する必要があるときは、当該情報に係る業務を主管する所属の長及び当該情報を取り扱う警察情報システムに係るシステムセキュリティ責任者と協議の上、必要な見直しを行わなければならない。

4　情報の取扱い

(1)　一般的な措置

情報の取扱いについては、アからエに規定するもののほか、兵庫県警察文書管理規程（平成13年兵庫県警察本部告示第520号）、兵庫県警察における文書の管理に関する訓令（平成13年兵庫県警察本部訓令第14号）及び兵庫県警察文書管理規程等の解釈及び運用要領（平成13年兵警総例規甲第14号）並びに兵庫県警察職員勤務規程（昭和30年兵庫県警察本部訓令第29号）に定めるところによる。

ア　情報の作成、入手及び利用

(ｱ)　警察職員は、情報を不正に作成し、利用し、又は処分し、若しくはき損してはならない。

(ｲ)　警察職員は、情報を不当な目的で入手し、複製し、又は他の者に提供してはならない。

(ｳ)　警察職員は、情報を警察の庁舎外に不正に持ち出してはならない。

(ｴ)　警察職員は、情報セキュリティ管理者が認めたときを除き、情報の分類を他の者が認識できる方法により明示しなければならない。

イ　情報の管理

警察職員は、取り扱う情報の分類の区分に応じ、警察情報システム等、外部記録媒体、ドキュメント及び入出力資料の紛失及び盗難の防止に対して十分に配意し、適切に管理しなければならない。

ウ　情報の提供

(ｱ)　警察職員は、情報を公開するときは、当該情報が別表１において機密性低に分類される情報であることを確認しなければならない。

(ｲ)　警察職員は、情報を電磁的記録により公開し、又は提供するときは、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置をとらなければならない。

エ　情報の消去

(ｱ)　システムセキュリティ責任者は、電子計算機若しくはネットワーク機器を廃棄し、又はその利用を終了するときは、システム管理担当者又はネットワーク管理担当者に、データ消去ソフトウェア又はデータ消去装置の利用、物理的又は磁気的な破壊等の方法により、これらに保存された全ての情報を復元できないように措置させなければならない。この場合におい

て、システムセキュリティ責任者又はシステムセキュリティ維持管理者は、当該措置が確実にとられたことを確認しなければならない。

(ｲ)　システムセキュリティ維持管理者又は運用管理責任者は、警察職員が、電子計算機、ネットワーク機器又は外部記録媒体を他の者へ提供しようとするときは、これらに保存された情報を復元できない状態にする必要性の有無を検討し、必要があると認めた情報については、当該警察職員に、データ消去ソフトウェア、データ消去装置等により、当該情報を復元できないように措置させなければならない。この場合において、システムセキュリティ維持管理者又は運用管理責任者は、当該措置が確実にとられたことを確認しなければならない。

(ｳ)　警察職員は、情報を廃棄するときは、裁断、データの消去等の方法により当該情報を復元できないように措置しなければならない。

(2)　情報の分類に応じた措置

情報の分類の区分に応じた措置は、別表２のとおり行う。

第４　警察情報システム等の構成要素についての対策

１　設置環境、維持管理等

(1)　別表１において機密性高若しくは機密性中に分類される情報に係るデータベース装置若しくはネットワーク機器（施錠された筐体に収容されているものであって電気通信回線から切り離されたときに直ちにそのことが検知できる仕組みを有するもの及び電子計算機（データベース装置を除く。(2)において同じ。）に近接して設置する必要のあるネットワーク機器を除く。）を設置し、又はそれらの装置若しくは機器に係るシステムドキュメントを保管する室（以下「警察情報システム機械室等」という。）は、人及び物の出入りを確実に管理することができ、外部からの侵入及び内部の視認が容易にできない構造の区域としなければならない。また、警察情報システム機械室等には、立入りが認められた者以外の者が立ち入ることができないよう必要な措置をとらなければならない。

(2)　別表１において機密性低、完全性低及び可用性低に分類される情報以外の情報（以下「要保護情報」という。）を取り扱う電子計算機を設置し、それらの機器に係るシステムドキュメントを保管し、又は要保護情報に係る入出力資料及び外部記録媒体を取り扱う場所は、人及び物の出入りを管理することができるように区画された区域とし、電子計算機の画面、システムドキュメント及び入出力資料をその区域の外から視認することができない構造としなければならない。また、その区域には、立入りが認められた者以外の者が立ち入ることができないよう必要な措置をとらなければならない。

(3)　情報セキュリティ管理者は、警察情報システム機械室等に立ち入ることができる者の範囲をあらかじめ定め、システムセキュリティ維持管理者又は運用管理責任者は、そのうち、必要な者に許可を与えなければならない。また、警察職員以外の者が警察情報システム機械室等に立ち入るときは、警察職員を立ち会わせなければならない。

(4)　警察情報システム機械室等に設置されている警察情報システムを構成する機器、外部記録媒体及びシステムドキュメントを警察情報システム機械室等の外に持ち出そうとする者は、システム管理担当者又はネットワーク管理担当者の立会いの下でこれを行い、その状況を記録しなければならない。

(5)　システムセキュリティ維持管理者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等に必要なドキュメント及びその内容を記録するための簿冊を整備し、それらの内容を常に最新のものとしておかなければならない。

(6)　システム管理担当者及びネットワーク管理担当者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等に必要な作業（軽微なものを除く。）を行うに当たっては、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行わなければならない。

(7)　情報セキュリティ管理者は、警察情報システムについて、一元的に管理するため、必要な事項を記載した台帳を整備しなければならない。

2　電子計算機

(1)　共通対策

ア　警察職員は、警察情報システム等を構成する機器、外部記録媒体及びドキュメントを適正に管理しなければならない。

イ　警察職員は、警察情報システム等を構成する機器、外部記録媒体及びドキュメントを他の者に不正に交付し、又は利用させてはならない。

ウ　警察職員は、警察情報システム等を構成する機器及び外部記録媒体として、個人所有の機器及び外部記録媒体を利用してはならない。

エ　警察職員は、あらかじめ定められた目的以外の目的で不正に警察情報システム等を利用してはならない。

オ　警察職員は、電子計算機を利用して警察の業務に係る情報の管理その他の情報の処理を行おうとするときは、運用管理責任者が認めたときを除き、警察の業務に関する情報の管理その他の情報の処理を目的として整備された警察情報システム等以外のものを利用してはならない。

カ　警察職員は、情報セキュリティ管理者が認めたときを除き、警察情報システムを構成する機器に電子計算機等を接続し、若しくは増設し、又は警察情報システムを構成する機器を交換してはならない。

キ　警察職員は、システムセキュリティ責任者が認めたときを除き、警察情報システムを構成する機器の改造を行い、又はソフトウェアの追加、削除若しくは変更をしてはならない。

ク　警察職員は、違法性及び危険性の生ずるおそれのあるファイル共有ソフト等のソフトウエアを警察情報システム等において使用してはならない。

ケ　警察職員は、警察情報システム等を構成する機器及び外部記録媒体を警察の庁舎外に持ち出すときは、別に定める場合を除き、情報セキュリティ管理者の承認を受けなければならない。

コ　システムセキュリティ責任者は、電子計算機（データベース装置を除く。）について、不正な利用の防止等を図るための必要な対策をとらなければならない。

サ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、データベース装置について、許可のない者が容易に操作できないようにするための必要な措置をとらなければならない。

シ　システムセキュリティ責任者は、電気通信回線を経由してデータベース装置の保守作業を行う場合において、送受信される情報を暗号化する機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けなければならない。この場合において、システムセキュリティ維持管理者は、送受信される情報を暗号化する必要性を検討し、必要があると認めたときは、暗号化しなければならない。

ス　システムセキュリティ責任者は、電子計算機へのインストールを認めるソフトウェア及び警察情報システム等の維持管理に利用するソフトウェアを定めなければならない。

セ　システムセキュリティ維持管理者は、前記スの規定によりシステムセキュリティ責任者が定めたソフトウェア以外のものが稼働していることを認知したときは、当該ソフトウェアを停止しなければならない。また、利用を認めたソフトウェアであっても、利用しない機能は無効化しなければならない。

ソ　システムセキュリティ責任者は、警察情報システム等について、盗難及び設置場所からの不正な持ち出しを防止するための措置をとらなければならない。

タ　システム管理担当者は、データベース装置の時刻設定を正確なものとしなければならない。

(2)　持ち出し用パソコン対策

ア　システムセキュリティ責任者は、持ち出し用パソコンについて、不正な利用の防止等を図るための必要な対策をとらなければならない。

イ　警察職員は、持ち出し用パソコンを警察の庁舎外に持ち出す必要があるときは、持ち出し期間を明らかにして、運用管理責任者の承認を受けなければならない。また、持ち出しを終了したときは、その旨を報告しなければならない。

ウ　運用管理責任者は、警察職員が、持ち出し用パソコンを警察の庁舎外に持ち出した場合において、持ち出し期間を満了しているにもかかわらず終了の報告がないときは、その状況を確認し、必要な対応を講じなければならない。

エ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、持ち出し用パソコンから無線回線を利用して警察情報システムにアクセスする仕組みを構築してはならない。

3　電子メール及びウェブ

(1)　警察職員は、職務の遂行に係る情報を電子メールにより送受信するときは、

警察の運営又は外部委託に係る電子メール機能を利用しなければならない。この場合において、受信した電子メールについては、適切な方法により当該内容を表示しなければならない。

(2)　システムセキュリティ責任者は、電子メールの送受信時に認証を行う機能を設けなければならない。

(3)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電子メールを保管、送受信又は中継するために設置される電子計算機及びウェブサービスを提供するために設置される電子計算機を不正に使用されることのないように構築し、及び管理しなければならない。

(4)　警察職員及びシステムセキュリティ責任者は、電子メール機能の利用及びウェブサービスの提供に当たっては、利用者の情報セキュリティが損なわれることのないように必要な措置をとらなければならない。この場合において、警察職員以外の者に電子メールの送信又はウェブサービスの提供をするときは、情報セキュリティ管理者が認めたときを除き、警察機関であることが保証されるドメイン名を使用しなければならない。

4　電気通信回線

(1)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電気通信回線を利用するに当たっては、当該接続により情報セキュリティの維持に及ぼす影響を検討しなければならない。

(2)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等を構成する電気通信回線として、情報セキュリティ管理者が認めた回線を利用しなければならない。

(3)　警察職員は、情報セキュリティ管理者が認めたときを除き、警察情報システム等を構成する機器を外部回線に接続し、又は外部回線から警察情報システム等にアクセスする仕組みを構築してはならない。

(4)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、ネットワーク機器について、許可のない者が容易に操作できないようにするための必要な措置をとらなければならない。

(5)　ネットワーク管理担当者は、ネットワーク機器の時刻設定を正確なものとしなければならない。

(6)　ネットワーク管理担当者は、警察情報システムを構成する電気通信回線の監視をシステム管理担当者と協力して行わなければならない。この場合において、監視により得られた結果については、消去又は改ざんが行われないように管理しなければならない。

第５　情報セキュリティ要件の明確化に基づく対策

１　情報セキュリティについての機能

(1)　アクセス制御機能等

ア　システムセキュリティ責任者は、アクセス権者以外の者によるアクセス及びアクセス権者によるアクセス範囲を越えたアクセスを防止するために、整備する警察情報システムごとに認証、アクセス制御及び権限管理を行う機能

を設けなければならない。

イ　システムセキュリティ責任者は、アクセス権者及び各アクセス権者のアクセス範囲を定めるときは、当該警察情報システムで取り扱う情報に係る業務を主管する所属の長と協議の上、整備する警察情報システムごとに必要な手続を明確化し、業務上の責務と必要性を勘案して、必要最小限の範囲に限らなければならない。

ウ　運用管理責任者は、所属の警察情報システムのアクセス権者及びアクセス範囲を適正に管理しなければならない。

エ　警察職員は、自己のユーザＩＤ以外のユーザＩＤを用いて、警察情報システムを利用してはならない。

オ　警察職員は、自己のユーザＩＤ及びパスワード（以下「ユーザＩＤ等」という。）を他の者に知られることのないように適切に管理しなければならない。ただし、人事異動、長期休暇等に伴う引継ぎのために特に設定したユーザＩＤ等及びあらかじめ複数の者が共用することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。

カ　警察職員は、認証に用いるＩＣカード等について、本人が意図しない使用、紛失等のないように適切に管理しなければならない。

キ　警察職員は、認証に用いるＩＣカード等を他の者に付与し、又は貸与してはならない。ただし、あらかじめ複数の者が共有することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。

ク　警察職員は、認証に用いるＩＣカード等を利用する必要がなくなったときは、これをシステムセキュリティ維持管理者に返納するなどの適切な措置をとらなければならない。

ケ　警察職員は、警察情報システムに設けられた機能を用いて、当該警察情報システムに保存される情報の分類の区分に従い、必要なアクセス制御の設定をしなければならない。

コ　システムセキュリティ維持管理者は、遠隔地から制御又は監視する警察情報システムについて、権限のない者が遠隔地から当該機器の制御又は監視を行うことがないよう厳重に管理しなければならない。

サ　システムセキュリティ維持管理者は、システム管理担当者及びネットワーク管理担当者の権限を個別の者に付与しなければならない。また、これを他の職員に代理させることはできない。

(2)　証跡管理

ア　システムセキュリティ責任者は、警察情報システム等について、情報セキュリティ管理者が認めたときを除き、証跡を取得する機能を設けなければならない。

イ　システムセキュリティ維持管理者は、警察情報システム等に設けられた機能を利用して、事象ごとに必要な項目を証跡として記録し、及び管理すると

ともに、当該記録を必要に応じて分析し、適切な措置をとらなければならない。

ウ　システムセキュリティ維持管理者は、システム管理担当者、ネットワーク管理担当者及び警察職員に対して、証跡の管理、分析等を行う可能性があることをあらかじめ周知しなければならない。

(3)　暗号と電子署名

ア　情報セキュリティ管理者は、暗号化又は電子署名の付与に用いるアルゴリズムを、警察庁が定める守秘用暗号から選定するとともに、使用されている暗号の安全性を随時評価して、必要な変更を行わなければならない。

イ　システムセキュリティ責任者は、警察情報システム等において暗号化又は電子署名の付与に用いるアルゴリズムを前記アの規定により情報セキュリティ管理者が選定したものから選定しなければならない。

ウ　システムセキュリティ維持管理者は、電子署名の付与を行う必要があると認めた警察情報システム等について、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供しなければならない。

エ　警察職員は、システムセキュリティ責任者が定めるところにより、暗号化された情報の復号又は電子署名の付与に用いる鍵の管理を適切に行わなければならない。

2　特定脅威等への対策

(1)　セキュリティホール対策

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、電子計算機及びネットワーク機器の構築及び運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールについて対策を講じなければならない。

イ　システム管理担当者及びネットワーク管理担当者は、管理の対象となる電子計算機及びネットワーク機器に関連する公開されたセキュリティホールの情報の入手に努めなければならない。この場合において、その情報を入手したときは、システムセキュリティ責任者及びシステムセキュリティ維持管理者に報告しなければならない。

ウ　システムセキュリティ責任者は、入手したセキュリティホールに関連する情報から、当該セキュリティホールが、警察情報システム等に及ぼす影響を分析した上で、セキュリティホール対策計画を作成し、これに基づいたセキュリティホール対策を講ずるとともに、随時警察職員に周知しなければならない。

エ　システムセキュリティ維持管理者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を記録するとともに、これを分析し、不適切な状態にある電子計算機及びネットワーク機器を把握したときは、適切に対処しなければならない。

オ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、入手したセキュリティホールに関連する情報及び対策方法について、必要に応

じ、他のシステムセキュリティ責任者及びシステムセキュリティ維持管理者と共有しなければならない。

(2)　不正プログラム対策

ア　警察職員は、コンピュータ・ウイルス等不正プログラムが電子計算機及び外部記録媒体に存在していないことを確認しなければならない。この場合において、不正プログラムが発見されたときは、直ちに拡散の防止のための措置をとらなければならない。

イ　情報セキュリティ管理者は、不正プログラムの感染を回避するために警察職員が留意しなければならない事項及び日常的に実施しなければならない事項を定め、これを警察職員に周知しなければならない。

ウ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、不正プログラムから電子計算機を保護するために必要な対策を講じなければならない。

エ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、前記ウの規定により講じた対策の状況を適宜把握し、必要な見直しを行わなければならない。

(3)　IPv6通信への対策

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システムにIPv6技術を利用する通信（以下「IPv6通信」という。）の機能を導入するときは、他の警察情報システムの情報セキュリティが損なわれることのないように必要な措置をとらなければならない。

イ　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、IPv6通信を想定していない電気通信回線に接続する全ての電子計算機及びネットワーク機器について、IPv6通信を停止するための機能を有している場合には、当該機能の設定を適切に行わなければならない。

(4)　踏み台対策

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、外部回線に接続する警察情報システム等が、不正アクセス等の中継地点として使用されることを防止するため、前記(1)及び(2)に規定するもののほか、必要な措置をとらなければならない。この場合において、不正アクセス等の中継地点として使用されたときの影響が最小となるように警察情報システム等を構築しなければならない。

3　警察情報システム等の情報セキュリティ要件

(1)　警察情報システム等の計画及び設計

ア　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等について、その構築から運用管理にわたり、情報セキュリティを維持するための支援を情報セキュリティ管理者に求めることができる。

イ　システムセキュリティ責任者は、警察情報システム等の情報セキュリティ要件を決定し、その要件を満たすために、機器等の購入（購入に準ずる賃貸

借契約を含む。）及びプログラム開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティに対する脅威への対策並びに警察情報システム等の構成要素についての対策について定めなければならない。

ウ　システムセキュリティ責任者は、構築する警察情報システムに重要な情報セキュリティ要件があると認めたときは、当該警察情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書のＳＴ評価・ＳＴ確認を受けなければならない。ただし、警察情報システムを改修する場合であって、見直し後のセキュリティ設計仕様書において重要な情報セキュリティ要件の変更が軽微であると認めたときは、この限りでない。

エ　システムセキュリティ責任者は、構築した警察情報システムの運用を開始するに当たって、情報セキュリティの観点から運用開始のための手順及び環境を定めなければならない。

(2)　警察情報システム等の情報セキュリティ要件

ア　警察情報システム等の構築、運用及び監視

　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等の構築、運用及び監視に際しては、情報セキュリティ要件に基づき定めた情報セキュリティ対策を行わなければならない。

イ　警察情報システムの移行又は廃棄

　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システムの移行又は廃棄を行うときは、情報の消去及び保存並びに警察情報システムの再利用についての必要性を検討し、適切な措置をとらなければならない。

ウ　警察情報システム等の見直し

　システムセキュリティ責任者は、警察情報システム等の情報セキュリティ対策について見直しを行う必要性の有無を適宜検討し、必要があると認めたときはその見直しを行い、必要な措置をとらなければならない。

4　外部委託

(1)　システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理責任者は、警察情報システム等の開発、運用管理、維持管理等を外部委託するときは、当該委託によって情報セキュリティが損なわれることのないよう、十分に検討の上、委託先には事業の継続性を有すると認められる事業者を選定しなければならない。

(2)　システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理責任者は、警察情報システム等の開発、運用管理、維持管理等を外部委託するときは、あらかじめ当該委託に係る作業を監督する警察職員の任務を定めるとともに、当該委託に係る業務の実施の場所及び方法、当該委託に係る業務に従事する者の範囲、委託先によるアクセスを認める範囲その他警察情報システム等の情報セキュリティの観点から委託の相手方に遵守させるべき事項を明記した仕様書等を作成しなければならない。また、契約に当たっては、当該事項

を遵守させるための措置を定めるなど情報セキュリティの維持に関し必要な措置をとらなければならない。

(3)　システムセキュリティ責任者及びシステムセキュリティ維持管理者は、警察情報システム等に係る仕様書で一般に公開されるものを作成するときは、当該仕様書が情報セキュリティの観点から支障のないものであることについて、情報セキュリティ副管理者の確認を受けなければならない。

5　業務継続計画との整合的運用の確保

情報セキュリティ管理者、システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理責任者は、業務継続計画（優先度が高い業務の継続性を確保するために必要な事項を定めたものをいう。以下同じ。）を策定するときは、業務継続計画と兵庫県警察情報セキュリティポリシーの整合的な運用が可能となるよう必要な措置をとらなければならない。

第６　事案発生時の措置

1　対処方法等の策定及び周知

情報セキュリティ管理者は、障害、事故等の事案について、その態様、対処方法、連絡体制、報告手順等当該事案を迅速かつ的確に措置するために必要な事項を定め、警察職員に周知しなければならない。

2　警察職員等の責務

システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理責任者並びに警察職員は、障害、事故等の事案発生時に、情報セキュリティ管理者が定める事項に基づき、必要な措置をとらなければならない。

3　事案の原因調査と再発防止策

(1)　情報セキュリティ管理者は、障害、事故等の事案が発生したときは、当該事案の原因を調査し、再発防止策を策定しなければならない。

(2)　情報セキュリティ管理者は、前記(1)の規定による調査をした場合において、当該事案の重要性にかんがみ、その調査結果を報告する必要があると認めるときは、警察本部長及び最高情報セキュリティ管理者に報告しなければならない。この場合において、最高情報セキュリティ管理者に報告するときは、警察庁情報セキュリティ管理者を通じて行うものとする。

(3)　情報セキュリティ管理者は、システムセキュリティ責任者、システムセキュリティ維持管理者又は運用管理責任者から障害、事故等についての報告を受けたときは、その内容を検討し、再発防止策を実施するための必要な措置をとらなければならない。

4　兵庫県警察情報セキュリティポリシー違反時の対応

(1)　情報セキュリティ管理者は、警察職員が兵庫県警察情報セキュリティポリシーに違反して警察情報システム等を使用したときは、期間を定め、その警察職員に警察情報システム等を使用させないことができる。

(2)　情報セキュリティ管理者は、警察情報システムと接続されている電子計算機が、兵庫県警察情報セキュリティポリシーに違反していることが明らかになったときは、当該電子計算機との接続を停止することができる。

第７　自己点検及び教養

１　自己点検

(1)　情報セキュリティ管理者は、情報セキュリティの維持のために警察職員が実施しなければならない事項について、その実施状況を自己点検するための年度ごとの実施計画及び実施手順を定めるものとする。

(2)　警察職員は、前記(1)の規定により定められた実施計画及び実施手順に基づき、自己点検を実施するものとする。

２　教養

情報セキュリティ管理者は、兵庫県警察情報セキュリティポリシーを正しく理解し、これを確実に実施するために必要な教養を警察職員に対して行わなければならない。

第８　その他

１　兵庫県警察情報セキュリティポリシーに係る情報の管理

兵庫県警察情報セキュリティポリシーのうち、公知となることによって、警察情報システム等に係る犯罪、不正行為等による情報の漏えいその他の情報セキュリティの侵害事案の発生が懸念され、又は既存の警察情報システム等に新たな情報セキュリティに係る対策を講ずる必要が生じるものについては、部外に公開してはならない。

２　兵庫県警察情報セキュリティポリシーの見直し

兵庫県警察情報セキュリティポリシーの内容については、見直しを行う必要性の有無を適宜検討し、必要があると認めたときはその見直しを行わなければならない。

３　例外措置の適用

情報セキュリティ管理者は、兵庫県警察情報セキュリティポリシーに定める情報セキュリティの維持に関する事項を遵守することが困難であると認める場合において、業務遂行上やむを得ない合理的な理由のあるときは、当該事項と異なる代替の措置を講ずること又は当該事項の適用を除外することを承認することができる。

４　細目事項に関する委任

警察情報システム等に係る情報セキュリティの維持に関し必要な細目事項は、総務部長が定める。

別表１　情報の分類

１　機密性の分類

分類	情報の種類
機密性高	警察情報システム等において取り扱われる情報のうち、秘密文書（兵庫県警察における秘密文書の取扱いに関する訓令（平成13年兵庫県警察本部訓令第20号）第２条第１項に規定する秘密文書をいう。）の内容に相当する情報その他の機密性が損なわれることによる影響が大きいもの
機密性中	警察情報システム等において取り扱われる情報のうち、直ちに一般に公開することを前提としていないもの
機密性低	警察情報システム等において取り扱われる情報のうち、機密性高又は機密性中に分類される情報以外のもの

２　完全性の分類

分類	情報の種類
完全性高	警察情報システム等において取り扱われる情報（書面を除く。）のうち、改ざん又は滅失した場合に業務の的確な遂行に支障を及ぼすおそれがあるもの
完全性低	警察情報システム等において取り扱われる情報（書面を除く。）のうち、完全性高に分類される情報以外のもの

３　可用性の分類

分類	情報の種類
可用性高	警察情報システム等において取り扱われる情報（書面を除く。）のうち、その情報が使用できないときに業務の安定的な遂行に支障を及ぼすおそれがあるもの
可用性低	警察情報システム等において取り扱われる情報（書面を除く。）のうち、可用性高に分類される情報以外のもの

別表２　情報の分類に応じた措置

分類	遵守事項	
	警察職員	情報セキュリティ管理者等
要保護情報 （機密性高） （機密性中） （完全性高） （可用性高）	1　情報を放置してはならない。 2　情報を不正に警察の庁舎外に持ち出してはならない。 3　情報を取り扱う警察情報システム等を構成する機器若しくは情報を記録した外部記録媒体を警察の庁舎外へ持ち出すとき、又は警察の庁舎外で情報処理を行うときは、別に定める場合を除き、情報セキュリティ管理者の承認を受けるとともに、安全管理のために定められた措置をとらなければならない。 4　情報を移送するときは、安全の確保に留意して、送信又は運搬のいずれかの手段を決定し、運用管理責任者に届け出なければならない。 5　情報を部外に提供するときは、提供先において、当該情報が適切に取り扱われるための措置をとらなければならない。	（運用管理責任者） 1　情報を取り扱う警察情報システム等を構成する機器又は情報を記録した外部記録媒体を警察の庁舎外へ持ち出すときは、当該持ち出しに係る記録を取得しなければならない。 （システムセキュリティ維持管理者） 2　警察情報システム等又は外部記録媒体に保存された情報について、必要に応じて認証、アクセス制御及び権限管理を行わなければならない。 （システムセキュリティ責任者及び運用管理責任者） 3　情報セキュリティ管理者が認めたときを除き、情報を取り扱う警察情報システム等について、外部からの侵入、自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域に設置しなければならない。 4　情報を取り扱う持ち出し用パソコンは、アクセス制御等警察の庁舎内で利用する警察情報システム等と同等の対策が機能するように構成しなければならない。また、盗難を防止するための措置をとらなければならない。 5　情報を取り扱う警察情報システム等については、必要に応じて、取り扱う情報が適切なものであることを保証するための機能を設けなければならない。
要機密情報 （機密性高） （機密性中）	1　情報を必要以上に配付してはならない。 2　情報セキュリティ管理者が認めたときを除き、警察の庁舎外に設置されている機器に情報を保存してはならない。 3　情報セキュリティ管理者が認めたときを除き、外部回線に接続する警察情報システム等において、情報を取り扱っ	（運用管理責任者） 1　アクセス権者及びアクセス範囲について、必要に応じて見直しを行わなければならない。 （システムセキュリティ責任者） 2　情報を取り扱う警察情報システム等について、情報セキュリ

	てはならない。 4　情報を移送するとき、又は警察情報システム等若しくは外部記録媒体に情報を保存するときは、必要に応じて当該情報にパスワードを設定し、又は暗号化しなければならない。 5　持ち出し用パソコンを警察の庁舎外に持ち出すときは、利用環境に配意し、関係のない者に当該持ち出し用パソコンで取り扱う情報を視認されないようにしなければならない。	ティ管理者が認めたときを除き、暗号化を行う機能を設けなければならない。 3　情報を取り扱う持ち出し用パソコンについて、電磁的記録媒体に保存される情報の暗号化を行う機能を設けなければならない。
（機密性高）	1　情報を必要以上に複製してはならない。 2　情報を移送するとき、又は部外へ提供するときは、運用管理責任者の承認を受けなければならない。 3　情報セキュリティ管理者が認めたときを除き、警察職員が管理する警察情報システム等以外のものにおいて情報を取り扱ってはならない。	
（機密性中）	1　運用管理責任者が届出を要しないと定めたときを除き、情報を移送するとき、又は部外へ提供するときは、運用管理責任者に届け出なければならない。 2　運用管理責任者が認めたときを除き、警察職員が管理する警察情報システム等以外のものにおいて情報を取り扱ってはならない。	
要保全情報（完全性高）	1　情報が事実と合致するよう、情報入力時における確認、臨時の点検、補正等の措置を確実に実施しなければならない。 2　情報を移送するとき、又は警察情報システム等若しくは外部記録媒体に情報を保存するときは、必要に応じて電子署名の付与又はバックアップを取得し、若しくは複写しなければならない。	（システムセキュリティ責任者） 1　情報を取り扱う警察情報システム等について、電子署名の付与又は検証を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けなければならない。 2　情報を取り扱う警察情報システム等、外部記録媒体及びドキュメントについて、必要に応じてバックアップを取得し、又は複写した上で、適切に保管しなければならない。
要安定情報（可用性高）	情報を移送するときは、必要に応じて、同一の情報を異なる経路及び手段で移送するなど適切な措置をとらなければな	（システムセキュリティ責任者） 1　情報を取り扱う警察情報システム等について、電子計算機に

	らない。	求められるシステム性能並びに電気通信回線及びネットワーク機器に求められる通信性能を、将来の見通しを含めて確保しなければならない。 2　情報を取り扱うデータベース装置について、必要に応じて冗長構成としなければならない。 3　情報を取り扱う警察情報システム等の設置に当たって、必要に応じて自然災害等に起因する障害を未然に防止する措置をとらなければならない。また、当該障害が発生したときの対応手順を定めなければならない。 4　情報を取り扱う警察情報システム等、外部記録媒体及びドキュメントについて、必要に応じてバックアップを取得し、又は複写した上で、適切に保管しなければならない。 5　情報を取り扱う警察情報システム等について、電気通信回線に与える負荷を評価するとともに、必要に応じて負荷を継続的に測定し、適切な措置をとらなければならない。 （システムセキュリティ維持管理者） 6　外部回線と接続して情報を取り扱う警察情報システム等について、電子計算機、電気通信回線及びネットワーク機器に設けられている機能をサービス不能攻撃対策に活用しなければならない。